IX kadencja

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji do Spraw Kontroli Państwowej (nr 124)**

z dnia 25 maja 2023 r.

Pełny zapis przebiegu posiedzenia

Komisji do Spraw Kontroli Państwowej (nr 124)

25 maja 2023 r.

Komisja do Spraw Kontroli Państwowej, obradująca pod przewodnictwem posła **Wojciecha Szaramy (PiS)**, przewodniczącego Komisji, oraz posła **Wojciecha Saługi (KO)**, zastępcy przewodniczącego Komisji, zrealizowała następujący porządek dzienny:

– rozpatrzenie Informacji Najwyższej Izby Kontroli o wynikach kontroli działań państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości.

W posiedzeniu udział wzięli: **Paweł Lewandowski** podsekretarz stanu w Ministerstwie Cyfryzacji wraz ze współpracownikami, **Tomasz Sordyl** p.o. dyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli wraz ze współpracownikami oraz **insp. Michał Pudło** zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości w Komendzie Głównej Policji.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Tadeusz Cieśluk** i **Tadeusz Oset** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Wojciech Saługa (KO):

Dzień dobry państwu. Otwieram posiedzenie Komisji do Spraw Kontroli Państwowej.

Na podstawie listy obecności stwierdzam kworum.

Przedmiotem dzisiejszego posiedzenia jest rozpatrzenie informacji Najwyższej Izby Kontroli o wynikach kontroli działań państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości.

Witam na posiedzeniu pana ministra Pawła Lewandowskiego, podsekretarza stanu w Ministerstwie Cyfryzacji, i przedstawicieli Najwyższej Izby Kontroli na czele z panem Tomaszem Sordylem, pełniącym obowiązki dyrektora Departamentu Porządku i Bezpieczeństwa Wewnętrznego.

Chciałbym zapytać państwa posłów, czy są uwagi do porządku dzisiejszego posiedzenia? Nie widzę. Stwierdzam, że porządek dzienny posiedzenia został przyjęty.

Prosiłbym teraz przedstawiciela Najwyższej Izby Kontroli o przedstawienie informacji.

Pełniący obowiązki dyrektor Departamentu Porządku i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli Tomasz Sordyl:

Dziękuję bardzo. Szanowny panie przewodniczący, szanowni państwo, dziękujemy za zaproszenie na posiedzenie Komisji. Razem z moimi współpracownikami zaprezentujemy wyniki kontroli działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości.

To kolejna kontrola NIK dotyczący obszaru z cyberbezpieczeństwa, tym razem koncentrująca się na kwestiach cyberprzestępczości. Od blisko 10 lat NIK bada zagadnienia związane z bezpieczeństwem wykorzystywania sieci internet, w szczególności w aspekcie działania poszczególnych organów państwa, których zadaniem jest ochrona naszego bezpieczeństwa. Obserwujemy, jak wiele zmieniło się na lepsze w tym obszarze na przestrzeni lat, również dzięki wnioskom i rekomendacjom Najwyższej Izby Kontroli, które są realizowane przez kontrolowane podmioty. Jeszcze 10 lat temu administracja państwowa ograniczała się w zasadzie do ochrony swoich własnych systemów. Działania były realizowane w sposób rozproszony, a świadomość istniejących zagrożeń i wyzwań z nimi związanych była na stosunkowo niskim poziomie.

To, że wiele zmieniło się na lepsze, nie oznacza jednak, że obecnie funkcjonujący system odpowiada już na wszystkie wyzwania. Nadal wiele pozostaje do zrobienia w tym obszarze, zwłaszcza że metody działania i narzędzia, wykorzystywane przez cyberprzestępców, również ciągle się rozwijają.

Doceniając wysiłek i zaangażowanie tysięcy pracowników administracji państwowej i samorządowej – funkcjonariuszy poszczególnych służb, którzy swoją codzienną pracą lub służbą dbają o minimalizowanie zagrożeń związanych z wykorzystaniem sieci internet dla naszego wspólnego bezpieczeństwa – pragniemy wskazać na obszary, które nadal wymagają poprawy.

Jeżeli pan przewodniczący pozwoli, to przekażę głos moim współpracownikom, którzy zaprezentują państwu szczegółowe wyniki kontroli.

Przewodniczący poseł Wojciech Saługa (KO):

Bardzo proszę, choć jeszcze nie przywitałem jednej branży. Jest z nami pan insp. Michał Pudło, zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości w Komendzie Głównej Policji.

Bardzo proszę.

Główny specjalista w Departamencie Porządku i Bezpieczeństwa Wewnętrznego Najwyższej Izby Kontroli Daniel Michalecki:

Dziękuję.

Dlaczego przeprowadziliśmy kontrolę? To jasne, że z roku na rok wzrasta aktywność Polaków w internecie. Niestety wzrasta też poziom przestępczości w sieci. Przeprowadzając kontrolę, której wyniki państwu prezentujemy, wyszliśmy z założenia, że państwo nie powinno zostawiać obywateli samych z problemem bezpieczeństwa w sieci. Tym bardziej, że aktywnie zaprasza obywateli do korzystania z internetu. W sieci działają dziś urzędy, platformy, usługi. W sieci można składać wnioski, załatwiać sprawy urzędowe. Państwo powinno wziąć odpowiedzialność za bezpieczeństwo poszczególnych obywateli w tym wirtualnym obszarze.

Doceniając wysiłek i zaangażowanie setek pracowników administracji – funkcjonariuszy poszczególnych służb, w tym pracowników Ministerstwa Cyfryzacji, Naukowej i Akademickiej Sieci Komputerowej, funkcjonariuszy Policji, których codzienne wysiłki przyczyniają się do zwiększania poziomu cyberbezpieczeństwa w naszym kraju – pragniemy wskazać na obszary, które, zgodnie z naszymi ustaleniami, wymagały i, przynajmniej częściowo, wymagają dalszej poprawy.

Co i kogo kontrolowaliśmy? Do kontroli wybraliśmy kluczowe podmioty realizujące zadania w zakresie zapobiegania i ograniczania skutków przestępstw internetowych – ministra cyfryzacji, pełnomocnika rządu do spraw cyberbezpieczeństwa, komendanta głównego Policji oraz dyrektora Naukowej i Akademickiej Sieci Komputerowej.

Podstawowe pytanie, które nam towarzyszyło, brzmiało – czy organy państwowe prowadzą adekwatne działania w celu identyfikowania, zapobiegania oraz ograniczania skutków przestępstw internetowych?

Jedno ważne zastrzeżenie i uzupełnienie – kontrola dotyczyła wybranych przestępstw popełnianych w cyberprzestrzeni, czyli takich, które narażały osoby fizyczne na straty finansowe lub prowadziły do takich strat. Chodzi o kradzież tożsamości – phishing. Nie zajmowaliśmy się w tej kontroli mową nienawiści czy zwalczaniem pedofilii. Skoncentrowaliśmy się na tym, czy indywidualni użytkownicy internetu są informowani na temat grożących im niebezpieczeństw, a w sytuacji, gdy staną się celem ataku, mogą liczyć na wsparcie właściwych instytucji państwowych.

Kontrolę rozpoczęliśmy z końcem 2021 r. W związku z tym przyjęliśmy, że przyjrzymy się działaniom wskazanych przed chwilą podmiotów w okresie 3 lat – od 2019 do 2021 r.

Proszę państwa, przedstawię ogólną ocenę naszej kontroli. Stwierdziliśmy, że – w kontrolowanym przez nas okresie – tworzony w Polsce system cyberbezpieczeństwa koncentrował się na wzmocnieniu bezpieczeństwa systemów uznawanych za kluczowe dla funkcjonowania państwa. I to dobrze. Jednak jego wadą było to, że pomijał, gdzieś gubił najliczniejszą grupę użytkowników internetu, którymi są osoby fizyczne. To w naszej ocenie było niewłaściwe. Tym bardziej, że prowadzona analiza ryzyka i monitoring

zagrożeń jednoznacznie wykazywały, że dominującą, gwałtownie zwiększającą się kategorią incydentów w cyberprzestrzeni były oszustwa komputerowe – w tym phishing, kradzież tożsamości – wymierzone w indywidualnych użytkowników sieci.

Zaniepokoiło nas i nie mogliśmy się z tym zgodzić, że, w okresie objętym kontrolą, dwa podstawowe organy odpowiedzialne za bezpieczeństwo cyberprzestrzeni, koordynację polityki rządu w tym obszarze – minister cyfryzacji i pełnomocnik rządu do spraw cyberbezpieczeństwa – nie reagowali na ryzyka oraz zagrożenia, nie dostosowywali do nich swoich działań organizacyjnych i informacyjnych. W ocenie tych organów cały obszar bezpieczeństwa obywateli w sieci oraz zagrożeń ze strony przestępczości internetowej pozostawał poza ich odpowiedzialnością. Nie widzieli konieczności podejmowania w tym zakresie działań, wskazując natomiast inne instytucje jako odpowiedzialne za ten obszar.

Opowiem syntetycznie o najważniejszych wynikach kontroli. Wszystkie podmioty, które skontrolowaliśmy, prowadziły regularną analizę ryzyka, analizę zdarzeń, zagrożeń, incydentów występujących w internecie. Pełnomocnik rządu do spraw cyberbezpieczeństwa od początku 2021 r. dostawał w układzie miesięcznym szczegółowe raporty z CSIRT NASK, w których wskazywano na rodzaj i skalę zagrożeń w sieci. Wyniki tych raportów, jak już mówiłem, były jednoznaczne. Wskazywały, że do 90% zdarzeń i incydentów w poszczególnych miesiącach to oszustwa komputerowe, phishing, dotykające indywidualnych użytkowników internetu.

Podczas gdy Policja i NASK reagowali lub przynajmniej próbowali reagować na wyniki tych analiz – mówimy o dostosowywaniu procedur działania, proponowaniu zmian strukturalnych czy legislacyjnych – to w przypadku tych dwóch kluczowych organów, a więc ministra cyfryzacji i pełnomocnika rządu, którzy mieli koordynować, spajać cały krajowy system cyberbezpieczeństwa, nie dostrzegliśmy skoordynowanych, zaplanowanych działań służących zapewnieniu bezpieczeństwa indywidualnym użytkownikom internetu.

Pełnomocnik i minister konsekwentnie budowali system cyberbezpieczeństwa ukierunkowany na instytucjonalnych interesariuszy, operatorów usług kluczowych, dostawców usług internetowych, samorząd, specjalistów IT. Gdzieś w tym wszystkim gubił się indywidualny użytkownik internetu.

Stwierdziliśmy, że obowiązujący podczas naszej kontroli dokument, jakim jest Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, wpisuje się w pewną niedobrą tradycję podobnych dokumentów w naszym kraju. Polityka Ochrony Cyberprzestrzeni RP z 2013 r., Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, czy wreszcie wspomniana przed chwilą strategia – wszystkie te dokumenty wykazują brak konkretów, co czyni z nich bardziej zbiór życzeń niż dokumenty, według których mają być podejmowane konkretne działania w sposób planowy, strategiczny w kontekście bezpieczeństwa całej cyberprzestrzeni. Nawet jeśli ochrona indywidualnych obywateli była wpisana w tę strategię, to, w kontrolowanym okresie, nic lub bardzo niewiele z tego wynikało.

Niestety po raz kolejny zidentyfikowaliśmy bolączkę administracji publicznej, na jaką cierpi ona od wielu lat, czyli brak zasobów, brak specjalistów, sprzętu, brak odpowiedniego oprogramowania. W przypadku Kancelarii Prezesa Rady Ministrów departament merytoryczny – który tak naprawdę powinien sterować, koordynować, sprawować pieczę nad systemem cyberbezpieczeństwa – pod koniec naszej kontroli liczył 21 pracowników i borykał się z potężnym problemem fluktuacji kadry. Ludzie pojawiali się w nim, znikali po krótkim czasie. Z pewnością tak wąski zespół osób – pomimo zaangażowania i kompetencji tych ludzi – nie był w stanie podołać wszystkim zadaniom. Taka była zresztą opinia wyrażona przez samego ministra i pełnomocnika rządu do spraw cyberbezpieczeństwa.

Problemy kadrowe i sprzętowe dotykały również Policji. W kontrolowanym okresie Policja nie miała wystarczającej liczby funkcjonariuszy, żeby zajmować się tematyką cyberbezpieczeństwa, a potrzeby sprzętowe czy softwarowe wydawały się przekraczać możliwości budżetowe tej formacji.

Trzeba jednak zauważyć, że kierownictwo Policji dostrzegło ten problem i podjęło działania zaradcze. Pod koniec 2021 r. została powołana zupełnie nowa, wyspecjalizowana jednostka organizacyjna – Centralne Biuro Zwalczania Cyberprzestępczości. Bardzo dobry, sensowny, zbieżny z naszymi przemyśleniami projekt. Podstawowe ryzyko, jakie zidentyfikowaliśmy,

jest oczywiste. Komendant główny Policji założył, że do końca 2025 r. uda mu się osiągnąć pełną operacyjność tej jednostki, czyli pozyskać prawie 2 tys. wysokiej klasy specjalistów. Znając specyfikę rynku IT i wysokość uposażeń na tym rynku – to może być trudne. Ale na pewno Policja powinna zrobić wszystko, by jednostka działała tak, jak to zostało zaplanowane i zamierzone.

Kolejny problem, szanowni państwo, to zgłaszanie przestępstw internetowych. Zidentyfikowaliśmy utrudnienia w zgłaszaniu tego rodzaju przestępstw przez obywateli. W przypadku Policji – która dla zdecydowanej większości osób jest pierwszym miejscem, gdzie można zgłaszać tego typu zdarzenia – nie opracowano procedur czy instrukcji dla obywatela, który pojawia się z takim specyficznym problemem. W przypadku funkcjonariuszy przyjmujących zgłoszenia wypracowano specjalne algorytmy działań. Miały one pomagać funkcjonariuszom, przede wszystkim tym nieposiadającym wiedzy specjalistycznej. Pomysł był bardzo dobry, jednak przy współpracy z ekspertem, biegłym, który wspierał nas w ramach tej kontroli, stwierdziliśmy, że algorytmy mają mankamenty. Nie były aktualizowane. Mimo wszystko, w naszej ocenie, ich stosowanie wymagało specjalistycznej wiedzy od policjantów.

Dobre, precyzyjne procedury wypracowano po stronie NASK. Tylko, że tu był inny problem. Z naszych badań wynikało, że tylko 1% obywateli wiedział, co to jest NASK, czym się zajmuje NASK, że tam jest zespół CSIRT, który może świadczyć wsparcie dla osób fizycznych, indywidualnych użytkowników sieci. Drodzy państwo, te ograniczenia spowodowały, że obywatele bardzo często rezygnowali z zawiadamiania właściwych organów, że stali się celem ataku przestępców internetowych.

Przyjrzeliśmy się także temu, jak państwo – poprzez swoje instytucje – podnosi poziom kompetencji obywateli, jak ich edukuje, jak ich ostrzega. Nasza ocena tych działań była, niestety, negatywna. Oceniliśmy je jako nierzetelne i nieskuteczne. Ważne jest, żeby wiedzieć, dlaczego. Po pierwsze stwierdziliśmy, że zabrakło jednolitego modelu informowania, edukowania obywateli. Zidentyfikowaliśmy sytuację, w której minister cyfryzacji od 2019 r. zaczął budować model, który określiliśmy jako scentralizowany. Od października 2019 r. w ramach rządowego portalu stworzył bazę wiedzy z zakresu cyberbezpieczeństwa. W tej bazie zamieszczono różne artykuły, ostrzeżenia, rekomendacje dla specjalistów, także dla osób fizycznych. Stworzono repozytorium wiedzy, gdzie m. in. my jako osoby fizyczne mogliśmy szukać informacji o zagrożeniach i wskazówek, jak mamy się zachować, kiedy takie zagrożenie się zmaterializuje.

Zgoła odmienną praktykę przyjął dyrektor NASK. Stworzył system – który nazwaliśmy systemem rozproszonym – różnych stron internetowych, portali. Problem jest taki, że NASK jest nadzorowany przez ministra cyfryzacji. W naszej ocenie aż prosiło się, by obie instytucje zaprezentowały jeden model – albo centralny, albo rozproszony.

Z kolei Policja docierała do obywateli poprzez informacje zawierane głównie w aktualnościach. Miały one, niestety, charakter migawki, doraźnej informacji, która pojawiała się i znikała. Można ją było wyszukać, ale było to utrudnione. Trzeba było użyć systemu tagów lub działającej wtedy niezbyt dobrze wyszukiwarki. Komendant główny zgodził się zresztą z nami, że budowa aktualizowanej bazy wiedzy trwałej jest dobrym pomysłem, który powinno zrealizować nowe biuro – Centralne Biuro Zwalczania Cyberprzestępczości (CBZC).

Kolejna sprawa. Jeśli chodzi o skuteczność działań edukacyjnych, to, niestety, one nie były bardzo skuteczne. Baza wiedzy na portalu *gov.pl* sprawiała wrażenie ukrytej. Niewiele osób wiedziało o jej istnieniu. Natomiast analiza wyświetleń poszczególnych zakładek czy artykułów pokazywała, że statystyki nie były oszałamiające – czy to jeśli chodzi o ministerialną bazę wiedzy, publikacje NASK czy Policji. Oczywiście były wyjątkowe publikacje, były nawet takie, które przeczytało i kliknęło 50 tys. osób. Jednak to były wyjątki.

Przede wszystkim, proszę państwa, żaden z kontrolowanych przez nas podmiotów nie dokonywał ewaluacji swoich publikacji pod kątem ich popularności i skuteczności. Warto podkreślić jeszcze raz ogromną aktywność NASK, działalność Policji, wielość publikacji i kampanii. Zabrakło prostego pytania – czy docieramy, trafiamy do obywateli? A jeśli nie, to co zrobić, żebyśmy dotarli i trafili do obywateli.

Kolejna rzecz. Zazwyczaj publikacje były, niestety, spóźnione wobec tego, co działo się w danym okresie w cyberprzestrzeni. W trakcie kontroli wybraliśmy sześć dużych kampanii phishingowych – a więc kampanii przestępczych z lat 2019–2021 – i zapytaliśmy ministra i pełnomocnika, czy ostrzegali obywateli, co im grozi. W przypadku czterech kampanii nie pokazano nam żadnych informacji zamieszczonych na stronach internetowych ministra. W przypadku dwóch pokazano nam bardzo luźno powiązane merytorycznie opracowania.

Statystyki odczytów tych publikacji nie były oszałamiające – 200–300 wyświetleń, czasami kilkadziesiąt osób przeczytało te informacje. To nie jest ten efekt, którego byśmy oczekiwali.

Konkluzja. W kontrolowanym przez nas okresie można było odnieść wrażenie, że państwo po prostu nie było widoczne w obszarze ostrzegania i edukowania obywateli. Miało się wrażenie, że dużo skuteczniej działał sektor komercyjny, który potrafił dotrzeć z bezpośrednimi komunikatami do swoich klientów. W sytuacji, gdy byliśmy bombardowani fałszywymi wiadomościami od rzekomych firm kurierskich, rzekomych banków, czy nawet rzekomych instytucji publicznych, w zasadzie jedynie prywatne firmy wysyłały skuteczne, bo docierające do użytkowników, alerty.

Chcąc uzupełnić wyniki naszej kontroli, zleciliśmy podmiotowi zewnętrznemu sporządzenie sondażu opinii publicznej w kierunku tego, na ile obywatele czują się poinformowani o zagrożeniach czyhających na nich w internecie i czy wiedzą, jak na nie reagować. Sondaż przeprowadzono zgodnie z zachowaniem wszystkich kanonów badań opinii publicznej na reprezentatywnej próbie tysiąca dorosłych osób. Warto podkreślić, że aż 404 osoby z tej grupy faktycznie zostały dotknięte atakami przestępców internetowych, komputerowych. Zlecone przez nas badanie potwierdziło, że duża część osób fizycznych nie wiedziała, co robić, ani gdzie się zgłosić w sytuacji ataku oszustów komputerowych. Ankietowani odpowiadali na przykład, że po skutecznie dokonanym na nich oszustwie internetowym nic nie zrobili, bo nie wiedzieli, co mają zrobić. Nie zgłaszali spraw, bo albo nie wiedzieli, że takie sprawy w ogóle można gdzieś zgłosić, albo nie wierzyli, że to coś da. Badanie tych 404 osób, które zostały dotknięte atakiem i zdecydowały się jednak zgłosić przestępstwo, wykazało, że tylko 2% spraw zakończyło się sukcesem, czyli wykryciem i skazaniem sprawcy lub odzyskaniem utraconych pieniędzy. W przypadku blisko 80% takich spraw ankietowani odpowiedzieli, że postępowanie zakończyło się, w sumie, niczym. Nie wiedzą, jak zakończyło się to postępowanie. Nie mają takiej wiedzy, nie mają takiej informacji.

Proszę państwa, podsumowując, przyzwyczailiśmy się myśleć o bezpieczeństwie państwa i jego obywateli w tradycyjny sposób – w wymiarze militarnym, w wymiarze zdrowia publicznego czy bezpieczeństwa wewnętrznego. Jednak chyba dla nas wszystkich jest jasne, że w XXI w. musimy dodać jeszcze jeden niezwykle ważny obszar bezpieczeństwa – cyberbezpieczeństwo. Obszar ten musi stać się jednym z priorytetów dla państwa polskiego, także jeśli chodzi o ochronę osób indywidualnych. Dlatego po naszej kontroli przedstawiliśmy kilka wniosków.

Pierwsze wnioski dotyczą zmian w prawie i obowiązujących strategiach, by w większym zakresie uwzględniały one bezpieczeństwo indywidualnych użytkowników internetu. Po drugie postulowaliśmy o wdrożenie jednolitego modelu edukowania obywateli na temat bezpieczeństwa w sieci – na przykład poprzez stworzenie rozpoznawalnego, oficjalnego państwowego serwisu zawierającego łatwo dostępne informacje na temat zagrożeń cyberbezpieczeństwa, trwających kampanii phishingowych, a także zaleceń i dobrych praktyk z zakresu tak zwanej cyberhigieny. Po trzecie wnioskowaliśmy o usprawnienie procesu przyjmowania zgłoszeń obywateli i instytucji w sprawie przestępstw internetowych – tak, żeby wiedzieli, gdzie i jak, żeby się nie bali, żeby się nie wstydzili z takimi sprawami zgłaszać się do odpowiednich organów.

Muszę na koniec powiedzieć, że cieszymy się, że znaleźliśmy w instytucjach, które kontrolowaliśmy, mimo oczywistych nieporozumień w procesie kontroli – takie się zdarzają – partnerów w zadaniu podnoszenia poziomu cyberbezpieczeństwa. Wskazują na to działania, jakie zostały podjęte już po zakończeniu naszej kontroli. Na podkreślenie zasługują: przygotowywany i procedowany projekt ustawy o zmianie niektórych ustaw w związku z zapobie-

ganiem kradzieży tożsamości przewidujący m.in.: możliwość skutecznego blokowania zaciągania zobowiązań; przygotowywany projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej przewidujący blokady wyłudzających wiadomości SMS oraz połączeń telefonicznych fałszujących numer abonenta; działania podejmowane w celu popularyzacji systemu S46; deklaracja komendanta głównego Policji o stworzeniu instrukcji postępowania dla ofiar cyberprzestępstw, instrukcji pomocnej przy zgłaszaniu przestępstw internetowych; prace nad dostosowaniem narodowych standardów cyberbezpieczeństwa do krajowych realiów, a przynajmniej myślenie o dostosowaniu.

Kampanie edukacyjne zaczęły być wreszcie widoczne. Ostatnim przykładem jest kampania zachęcająca do weryfikacji dwuetapowej. Dostrzegamy też zwrot ministra w myśleniu o odpowiedzialności za bezpieczeństwo osób fizycznych. Mam tu na myśli różne deklaracje, także te podczas niedawnej konferencji CyberGOV. Na dobrą sprawę, drodzy państwo, czy można skutecznie chronić instytucje, nie chroniąc indywidualnych użytkowników? Oni pracują w tych instytucjach. Ich słabość staje się słabością tych instytucji. Ich siła, świadomość, kompetencje chronią i wzmacniają te instytucje. Dziękuję bardzo.

Przewodniczący poseł Wojciech Szarama (PiS):

Dziękuję. Kto z państwa chciał zabrać głos? Proszę, panie pośle. Pan poseł Przemysław Koperski.

Poseł Przemysław Koperski (Lewica):

W tym sprawozdaniu, które pan przedstawił w raporcie, sygnalizował pan problemy dotyczące rekrutacji pracowników do nowego biura do walki z cyberprzestępczością. Tam docelowo miało być zatrudnione 2 tys. osób. Chciałem się dowiedzieć, czy sprawdzaliście, jaki jest na dzień dzisiejszy stan realizacji tego zatrudnienia? Kiedy ten wymagany poziom zostanie osiągnięty? Czy to też sprawdzaliście? Bo plany sobie, a mi chodzi o rzeczywistość. Dziękuję uprzejmie.

Przewodniczący poseł Wojciech Szarama (PiS):

Proszę. Pan poseł Ryszard Wilczyński.

Poseł Ryszard Wilczyński (KO):

Dziękuję bardzo za ten raport, bo jest chyba jednym z najważniejszych i najbardziej oczekiwanych dokumentów przez obywateli.

Nie ulega wątpliwości, że państwo ujawniliście rzecz nadzwyczaj przykrą – przez czas objęty kontrolą obywatele byli w zasadzie pozbawieni ochrony państwa. Taki jest generalny wniosek. To nie jest wniosek dobry dla partii rządzącej i dla władzy. Gdybym był członkiem obozu rządzącego, to płonąłbym ze wstydu. Koledzy rozmawiali cały czas, nie słuchali, a ja płonąłbym ze wstydu. Bo to, co pan przedstawił, jest porażające.

Na koniec rzeczywiście było troszkę słów, które napawają otuchą. Nawet pojawiła się jaskółka nadziei, że Policja trochę się wyłamała w tym wszystkim i zaczęła myśleć o obywatelach bardzo konstruktywnie, przygotowując się organizacyjnie do tego, żeby zmierzyć się z wyzwaniem. Tutaj należą się słowa szacunku dla Policji, bo tak należy. Mam nadzieję, że państwo doczekacie się silnego wzmocnienia w ramach ustaw modernizacyjnych Policji, aby dział walki z cyberprzestępczością był bardzo mocny. Tam są pieniądze. One powinny trafiać właśnie w te miejsca, gdzie jest najtrudniej. Zresztą podobno stworzono również ramy prawne, żeby fachowcy od IT, od cyberbezpieczeństwa zarabiali zdecydowanie więcej, nawet więcej niż sam komendant główny Policji. Podobno teraz tak jest i to cieszy. Chciałbym zauważyć, że rzeczywiście ustawa o przeciwdziałaniu kradzieży tożsamości jest procedowana.

Mam pytanie, na ile państwa wnioski rzeczywiście znalazły się w tym projekcie. I kolejne pytanie, na ile jest szansa, że rzeczywiście obywatel zobaczy, że jest jeden kanał zgłaszania przestępstw komputerowych czy informowania o dostrzeżonym zagrożeniu. Czy jest szansa? Bo jak widać, tych instytucji jest moc, natomiast nikt tego nie ogarnął. Podawał pan przykład NASK-u, który podejmował wiele działań, ale one były rozproszone. Tak samo – były działania, ale nie było ich ewaluacji i wyciągania wniosków. Czy jest realna szansa na to, że to się zmieni? Państwo, jak widzę, monitorujecie tę sytuację –

także po zakończeniu prac nad sprawozdaniem, nad raportem. Co z tego wynika? Co się zmieniło po waszych działaniach kontrolnych? Bardzo dziękuję.

Przewodniczący poseł Wojciech Szarama (PiS):

Pan przewodniczący Wojciech Saługa.

Poseł Wojciech Saługa (KO):

To kluczowa sprawa dla państwa polskiego na przyszłość. Absolutnie wszyscy powinniśmy się nad tym pochylić, posypać głowy popiołem, patrzeć też na to, co będzie w przyszłości.

Niejednokrotnie jako parlamentarzyści spotykamy się z tymi sprawami na przykład wskutek interwencji mieszkańców – tych bezradnych, tych 80%, którzy przychodzą i nie dostają żadnej pomocy. Sami też jesteśmy obiektami ataków. Większość posłów dostaje jakieś groźby o podłożeniu bomby czy jakieś groźby fizyczne. Mamy też kontakt z policją i reagujemy tak jak 80% społeczeństwa. Dzisiaj jest już taka znieczulica, że większość posłów tego nie zgłasza, bo więcej kosztuje zgłoszenie i przeprowadzenie tej procedury, która nic nie daje, niż machnięcie na to ręką i określenie ryzyka, czy to się wydarzy. Jeżeli widzimy, że policja jest bezbronna, to jak my, jako osoby fizyczne, jesteśmy bezbronni.

Trzeba zmienić podejście do tego, co się dzieje. Cyfrowy świat, sztuczna inteligencja, która nadchodzi, większość ludzi kompletnie tego nie rozumie. Państwo albo przejmie rolę zabezpieczenia obywateli przed różnymi gangsterami czy złymi ludźmi, albo polegniemy.

Ważne jest to, o czym powiedział pan poseł Wilczyński. Wiemy, ile mniej więcej zarabia informatyk. Wiemy, że cały czas borykamy z tym – chociażby na komisjach – że nie ma pieniędzy na fachowców. Jeżeli nie zdecydujemy się na najlepszych fachowców i nie nadrobimy straconego czasu, to ci wszyscy gangsterzy wyprzedzą nas z prędkością światła.

Dopiero tworzymy jakieś jednostki, coś tworzymy w Policji. Chodzimy też zeznawać na policję. Policja jest mocno niedoposażona, widzimy, na jakim pracuje sprzęcie, jakich ma fachowców. Cały system trzeba stworzyć od nowa i mocno trzymamy za to kciuki. Ten raport niech będzie kubłem zimnej wody. Oczekiwałbym od pana ministra i pana komendanta informacji, jakie działania przeprowadzamy, i czy jest jakieś światło w tunelu.

Jeszcze raz powtórzę – najgorzej wygląda ta statystyka, którą znamy z życia – większość ludzi nie wierzy w jakąkolwiek skuteczność Policji i rzecznika praw konsumenta. To się dzieje w różnych obszarach. Wszyscy rozkładają ręce i są bezbronni, a ci gangsterzy tylko hasają.

Czasami słyszę w Polskim Radiu, jak przestrzegają przed czymś emerytów. Wiemy jednak, że to niewiele daje. Na początek konieczna jest zmiana ustaw, blokowanie tych numerów.

Nam się wydaje, że państwo jest bezbronne wobec tych przestępstw, bo ich nie rozumie. Jak ich nie rozumie, to ich nie dostrzega. Jak ich nie dostrzega, to ich nie zwalcza. Takie może być przeświadczenie, ale zapewne chętnie posłuchamy pana ministra.

Przewodniczący poseł Wojciech Szarama (PiS):

Proszę się przedstawić.

Podsekretarz stanu w Ministerstwie Cyfryzacji Paweł Lewandowski:

Dziękuję bardzo. Paweł Lewandowski, podsekretarz stanu w Ministerstwie Cyfryzacji.

Panie przewodniczący, Wysoka Komisjo, dziękuję za udzielenie głosu. Przede wszystkim chciałbym zwrócić uwagę na to, że kontrolą objęto działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości, w latach 2019–2021.

Wyniki tej kontroli, jakkolwiek interesujące, dzisiaj można postrzegać z perspektywy historycznej. Nie uwzględniają zmian, jakie zaszły w ostatnich dwóch latach zarówno w obszarze rozwiązań legislacyjnych, jak i sytuacji międzynarodowej – przede wszystkim konfliktu zbrojnego na terytorium Ukrainy. Szczególnie ostatnia sytuacja pociąga za sobą nieustanną zmianę krajobrazu cyberzagrożeń, stąd też nieustanna aktywność ze strony ministra cyfryzacji oraz pełnomocnika rządu do spraw cyberbezpieczeństwa, podejmowanie wielu działań i inicjatyw mających na celu poprawę cyberbezpieczeństwa...

Poseł Ryszard Wilczyński (KO):

Gdyby pan mówił tak, żebyśmy nadążali ze słuchaniem. Pan, przepraszam, mamrocze… Pan mówi ważne rzeczy, ja to chcę docenić. Proszę mówić powoli i spokojnie, żebyśmy pana wysłuchali.

Przewodniczący poseł Wojciech Szarama (PiS):

Panie pośle, można zwrócić uwagę, ale proszę trochę grzeczniej.

Poseł Ryszard Wilczyński (KO):

Przepraszam, ale…

Przewodniczący poseł Wojciech Szarama (PiS):

Panie ministrze, proszę przysunąć mikrofon bliżej siebie i mówić troszkę głośniej.

Podsekretarz stanu w MC Paweł Lewandowski:

…stąd też nieustanna aktywność ze strony ministra cyfryzacji oraz pełnomocnika rządu do spraw cyberbezpieczeństwa, podejmowanie wielu działań i inicjatyw mających na celu poprawę cyberbezpieczeństwa, skuteczną obronę przed cyberatakami, podniesienie kompetencji cyfrowych obywateli oraz budowanie bezpiecznej i stabilnej infrastruktury cyberbezpieczeństwa.

Jedną z kluczowych inicjatyw, podjętych przez ministra cyfryzacji, jest projekt ustawy o zmianie niektórych ustaw w związku z zapobieganiem kradzieży tożsamości – to jest to zastrzeganie m.in. numeru PESEL. 22 maja 2023 r. projekt został skierowany do pierwszego czytania w komisjach. Projekt dotyczy zwiększenia ochrony przed nadużyciami wynikającymi z kradzieży danych i ograniczeniem skali zjawiska wyłudzania środków finansowych poprzez zaciąganie zobowiązań finansowych na inną osobę – m. in. umów kredytów i pożyczek czy sprzedaży nieruchomości – bez wiedzy i zgody właściciela. Dotyczy to także zjawiska tzw. SIM swappingu, czyli wyrobienia duplikatu karty SIM, która może być potem użyta do autoryzowania transakcji wykonanych przez złodzieja w instytucji finansowej.

Kolejnym bardzo ważnym krokiem – mającym na celu zapewnienie bezpieczeństwa użytkownikom – jest projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej. 7 marca projekt został skierowany do pierwszego czytania w Komisji Cyfryzacji, Innowacyjności, i Nowoczesnych Technologii. Jeszcze w czerwcu można spodziewać się sprawozdania Komisji o tym projekcie. Ustawa ma na celu zwiększenie poczucia bezpieczeństwa osób korzystających z usług komunikacji elektronicznej i faktycznego bezpieczeństwa korzystania z tych usług. Zgodnie z nowymi przepisami operatorzy będą musieli blokować SMS-y wyłudzające dane i połączenia głosowe, których celem jest podszywanie się pod inną osobę lub instytucje.

Odnosząc się bezpośrednio do informacji Najwyższej Izby Kontroli w części dotyczącej zarządzania systemem S46, należy podkreślić, że zadaniem systemu ma być wspieranie współpracy podmiotów wchodzących w skład Krajowego Systemu Cyberbezpieczeństwa, wśród których nie ma indywidualnych użytkowników internetu. Wynika to wprost z przepisów ustawy o Krajowym Systemie Cyberbezpieczeństwa.

System S46 nie jest systemem, który miałby bezpośrednio służyć zwalczaniu cyberprzestępczości skierowanej przeciwko indywidualnym użytkownikom internetu. Jednym z jego głównych założeń jest to, że wymiana informacji w tym systemie odbywa się nawet wtedy, gdy zakłócone będzie funkcjonowanie sieci internet lub publicznej sieci telefonicznej, a zatem nie będzie możliwości wykorzystania z poczty elektronicznej, formularzy zamieszczonych na stronach internetowych, usług telefonii głosowej i usług SMS. Ta funkcjonalność systemu S46 została w pełni osiągnięta.

Obecnie do systemu S46 podłączonych jest 49 podmiotów. Kolejne 50 podmiotów jest w trakcie podłączania. W trakcie podpisywania umów regulujących kwestie podłączenia do systemu jest kolejnych 86 podmiotów. Do podłączenia wytypowano również 410 innych podmiotów. Ponadto przepisy ustawy o Krajowym Systemie Cyberbezpieczeństwa nie obligują podmiotów Krajowego Systemu Cyberbezpieczeństwa do podłączenia się do systemu S46.

Departament Cyberbezpieczeństwa wraz z NASK zorganizował – i w dalszym ciągu organizuje – szereg spotkań warsztatowych z przedstawicielami podmiotów Krajowego Systemu Cyberbezpieczeństwa. Na warsztatach są omawiane korzyści wynikające z podłączenia się do systemu oraz zagadnienia organizacyjne i techniczne związane z podłączeniem się do systemu.

Istotną zmianą w podejściu do kwestii finansowania podłączenia danego podmiotu do systemu S46 było przerzucenie kosztów sprzętu niezbędnego do podłączenia na ministra cyfryzacji. Środki na ten cel pochodzą z dotacji celowej przyznawanej przez ministra cyfryzacji dla NASK, ze środków budżetu państwa na podstawie art. 47 ustawy o KSC. Z uwagi na ograniczenia wynikające z reguły wydatkowej, wskazanej w ustawie, środki dotacji celowej w związku ze skalą potrzeb okazały się niewystarczające. Już po zakończeniu kontroli NIK Naukowa i Akademicka Sieć K omputerowa pozyskała środki z Unii Europejskiej z programu REACT-EU, co pozwoli na sfinansowanie podłączeń 150 podmiotów – głównie operatorów usług kluczowych i podmiotów publicznych będących jednostkami samorządu terytorialnego – do końca 2023 r. Wraz z uruchomieniem środków z KPO przewidywane jest podłączenie do systemu kolejnych prawie 400 podmiotów – głównie operatorów usług kluczowych z sektora ochrony zdrowia oraz jednostek samorządu terytorialnego. Natomiast w złożonym przez ministra cyfryzacji projekcie nowelizacji ustawy o KSC jest zawarty przepis, który zobowiąże wybrane podmioty systemu do podłączenia się do systemu S46.

Poza działaniami legislacyjnymi, o których była mowa powyżej, minister – dążąc do podniesienia poziomu cyberbezpieczeństwa naszego kraju – podjął działania skierowane do podmiotów Krajowego Systemu Cyberbezpieczeństwa, w tym w dużej mierze do podmiotów administracji publicznej, które w ostatnim czasie stały się nieustannym celem ataków hakerów. W związku z tym do 31 maja w całym kraju obowiązuje trzeci stopień alarmowy CHARLIE-CRP oraz drugi stopień alarmowy BRAVO. W celu zapewnienia bezpiecznej komunikacji między podmiotami administracji publicznej powstał komunikator Threema, który jest darmowy dla użytkownika. Został skonfigurowany w sposób osobny na naszych własnych serwerach.

Innym działaniem jest – finansowana w ramach dotacji udzielonej przez ministra cyfryzacji – realizacja zadania zapewnienia usługi chmurowej ochrony przed atakami DDoS dla podmiotów realizujących zadania publiczne. Zadanie realizuje NASK i ma ono na celu ochronę przed atakami wolumetrycznymi DDoS. Warto podkreślić, że dla podmiotów objętych usługą ochrony w ramach przedmiotowego zadania usługa jest nieodpłatna. Z doświadczeń wynika, że usługa, o której mowa, dla wielu instytucji jest jedynym ratunkiem przed nasilającym się atakami.

Obserwujemy, że ataki na strony resortów siłowych są dwa razy częstsze niż odwiedziny strony przez zwyczajnych użytkowników internetu. Dla stron związanych z aktywnością zagraniczną polski współczynnik sięga rzędu 4–5. Podam dla przykładu, że w ciągu ostatniego tygodnia mechanizmy bezpieczeństwa zablokowały sumarycznie 480 tys. zdarzeń bezpieczeństwa, ponad 600 tys. ataków z wykorzystaniem botów. Obecnie 11 instytucji jest objęte pełną ochroną. Ochronę włączaną na życzenie ma 19 instytucji, 72 są szykowane do objęcia taką ochroną.

Istotne znaczenie w podnoszeniu poziomu cyberbezpieczeństwa odgrywają kampanie informacyjno-edukacyjne dotyczące cyberzagrożeń, przeciwdziałania im. Poruszają najczęstsze problemy, zagrożenia i oszustwa, jakie mogą spotkać użytkowników internetu.

Prowadzone kampanie przekładają się na podniesienie świadomości z zakresu cyberbezpieczeństwa obywateli, czego efektem jest wzrost liczby zgłoszonych incydentów. Rosnąca liczba zgłoszeń świadczy również o tym, że użytkownicy właściwie identyfikują CSIRT NASK jako instytucję, do której mogą się zwracać z wyzwaniami związanymi z zagrożeniami w sieci. To jest efekt kampanii. Emisje spotów, w których podkreślano wartość przesyłania podejrzanych SMS-ów do CSIRT NASK rozpoczęto w połowie listopada 2022 r. Kampania trwała do końca kwietnia tego roku. Przełożyło się to na wzrost liczby zgłoszeń w ujęciu miesięcznym. Warto zwrócić uwagę, że to emisje grudniowe realizowane w tzw. prime time – w przerwach i przed meczami polskiej reprezentacji w mistrzostwach świata w piłce nożnej – przyniosły najbardziej widoczne efekty. Za przykład niech posłużą emisję z 4 i 19 grudnia, które

wygenerowały kolejno 6870 i 7081 zgłoszeń. Tylko te dwa dni pozwoliły nam osiągnąć wynik lepszy niż w całym sierpniu czy kwietniu 2022 r.

Po zaobserwowaniu skuteczności tych działań postanowiono, że w 2023 r. będą realizowane reklamy adresowane do użytkowników promujące cyberbezpieczeństwo. Dwa tygodnie temu rozpoczęła się kampania zachęcająca do korzystania z weryfikacji dwuetapowej, a w przygotowaniu są kolejne projekty.

Ponadto planujemy kampanię społeczną skierowaną przede wszystkim do osób o niższych kompetencjach cyfrowych i mieszkańców mniejszych miejscowości. Grupę docelową stanowią dorośli Polacy. Kampania będzie obejmować reklamy telewizyjne, spoty, emisje w kinach. Zaplanowane jest też dotarcie do grupy docelowej przez reklamy zewnętrzne na lotniskach i dworcach. Kampania będzie realizowana także w internecie. Do zbudowania zasięgów kampanii planowana jest współpraca z wybranymi influencerami docierającymi do różnych grup społecznych. Jednym z priorytetów ministra cyfryzacji są działania mające na celu podnoszenie kompetencji z obszaru cyberbezpieczeństwa zarówno wśród podmiotów publicznych, jak i ogółu społeczeństwa. W niektórych z tych działań mogli państwo uczestniczyć osobiście. Właściwie to mam nawet listę, kto w nich uczestniczył. Zachęcam tych, którzy nie uczestniczyli, do tego, by wziąć w tym udział.

Pragnę podkreślić, że budowanie kompetencji użytkowników i świadomości zagrożeń to długotrwały proces, który, aby był skuteczny, musi być realizowany na wielu płaszczyznach. Mając na uwadze potrzebę podnoszenia kompetencji obywateli z obszaru cyberbezpieczeństwa, nie można zakładać, że wszystkie działania edukacyjne i informacyjne z tego obszaru będą uniwersalne i takie same dla każdego. Dlatego działania realizowane z inicjatywy ministra uwzględniają specyfikę różnych grup społecznych wśród użytkowników internetu.

Od 2022 r. w szkoleniach wzięło udział ponad 20 tys. osób. Podsumowując, do końca 2022 r. przeprowadzono 1448 szkoleń, w ramach których przeszkolono około 14 tys. osób. Szkolenia stacjonarne w ramach tego projektu są kontynuowane, a ich zasięg obejmuje obecnie cały kraj. Planuje się, że w ramach działań w 2023 r. zostanie przeprowadzonych 5 tys. szkoleń – aż czterokrotnie więcej niż na początku realizacji tego projektu.

Ponadto mamy cały szereg różnych szkoleń i kampanii, ale nie będę już o nich szczegółowo opowiadał, żeby nie zabierać państwu czasu. Jeżeli ktoś jest zainteresowany, to służę udostępnieniem materiału. Dziękuję państwu za uwagę.

Poseł Ryszard Wilczyński (KO):

Bardzo dziękuję. To, co pan powiedział, jest budujące. Mam nadzieję, że to rzeczywiście będzie jakościowa zmiana.

Proszę jeszcze wyjaśnić termin system S46, żebyśmy wiedzieli, o czym mówimy. Patrzyłem w słowniczku, ale nie znajduję takiego pojęcia. Pan mówił o jakimś systemie, do którego podłącza się stare podmioty. To jest wasz wewnętrzny język, nie mamy do niego dostępu, więc prosiłbym o wyjaśnienie.

Podsekretarz stanu w MC Paweł Lewandowski:

To jest system regulowany ustawą o krajowym systemie cyberbezpieczeństwa art. 46. Jest to system, który pozwala na funkcjonowanie podmiotów do niego podłączonych niezależnie od działania publicznych, jawnych sieci informatycznych i teleinformatycznych.

Poseł Ryszard Wilczyński (KO):

W czyjej gestii jest ten system?

Podsekretarz stanu w MC Paweł Lewandowski:

Ministra cyfryzacji.

Poseł Ryszard Wilczyński (KO):

Dziękuję.

Przewodniczący poseł Wojciech Szarama (PiS):

Pan poseł Koperski.

Poseł Przemysław Koperski (Lewica):

Panie przewodniczący, tylko przypominam, że nie dostałem odpowiedzi na zadane przeze mnie pytania.

Przewodniczący poseł Wojciech Szarama (PiS):

Proszę.

P.o. dyrektor departamentu NIK Tomasz Sordyl:

Przepraszam, pan przewodniczący udzielił głosu panu ministrowi, tak że teraz odpowiem na pytania kierowane do Najwyższej Izby Kontroli.

Jeżeli chodzi o pytania pana posła dotyczące rekrutacji specjalistów, to problem, tak jak podkreślaliśmy w naszej prezentacji, jest złożony. Są kłopoty z pozyskaniem specjalistów w tym zakresie.

Diagnozowaliśmy również taką sytuację, że część policjantów, którzy dotychchczas byli zatrudnieni w innych komórkach organizacyjnych Policji, przechodzi do nowo tworzonego biura, co powoduje efekt wysysania innych komórek, które nadal muszą realizować zadania i potrzebują specjalistycznego wsparcia. Na dzień dzisiejszy nie mamy informacji, ilu specjalistów udało się pozyskać. Może przedstawiciel komendanta głównego Policji będzie w stanie podać precyzyjnie dane.

Ze swojej strony mogę powiedzieć, że przyglądamy się kwestii tworzenia biura i rozważamy przeprowadzenie kontroli. Większość kontroli ma charakter ex post, czyli są przeprowadzane po zakończeniu jakiegoś procesu. Natomiast analizujemy kwestię, czy nie przeprowadzić kontroli towarzyszącej, którą możemy realizować równolegle z procesem tworzenia biura. Zakończyłaby się mniej więcej rok przed terminem wyznaczonym na utworzenie tego biura. Dzięki kontroli moglibyśmy dostarczyć komendantowi głównemu, państwu posłom i obywatelom informacje dotyczące przebiegu realizacji procesu tworzenia biura oraz wskazówki, rekomendacje dotyczące kontynuacji procesu, żeby zwiększyć szansę jego skutecznego zakończenia do 2025 r.

Jeżeli chodzi o pytanie pana posła Wilczyńskiego dotyczące projektu ustawy o kradzieży tożsamości, to pan minister wskazał na pewne elementy odnoszące się właśnie do tego, co będzie ujęte w tej ustawie i kolejnej ustawie dotyczącej ograniczenia zasięgu wszelkiego rodzaju kampanii phishingowych, wyłudzeń.

Dwa zastrzeżenia z naszej strony. Pierwsze – mówimy na razie o projektach ustaw. Mamy nadzieję, że one w tym czy innym kształcie zostaną uchwalone i będą skutecznym narzędziem do ograniczenia skali tej przestępczości, czy też przynajmniej niektórych ryzyk w zakresie tego zjawiska. One oczywiście nie są odpowiedzią na wszystkie postulaty, które przedstawialiśmy. Część z nich znalazła się jednak w ramach innych działań, o których wspomniał pan minister – mianowicie w kampaniach edukacyjnych. Uważamy je za bardzo istotny element realizowanych działań.

Świadomość obywateli, świadomość zagrożeń sprzyja zmniejszeniu skali tych zjawisk. Sprzyja również reakcji na sam fakt popełnienia przestępstwa, czyli choćby kwestii zabezpieczenia pewnych informacji, dostarczenia danych, które umożliwiłyby skuteczniejsze działanie organów ścigania. Na dzień dzisiejszy – nie jest to oczywiście tylko problem Polski – skala skuteczności tych działań nie jest zbyt wysoka.

Jeżeli chodzi o drugie pytanie – o szansę na to, czy to będzie jeden kanał informowania – wydaje mi się, że to pytanie jest bardziej skierowane do pana ministra. My ze swojej strony możemy powiedzieć, że mogą być realizowane różne modele. Każdy z tych modeli – system scentralizowany i system rozproszony – ma swoje wady i zalety. Natomiast jesteśmy przekonani, że powinno istnieć takie miejsce w internecie, które będzie miejscem pierwszego wyboru dla obywatela. Miejsce, do którego będzie mógł sięgnąć, uzyskując tam sprawdzone, wiarygodne, podane na czas informacje, które pomogą mu uniknąć zagrożeń czy ograniczyć skutki, w przypadku gdy stał się ofiarą przestępstwa wyłudzenia, czy innych zagrożeń, które płyną z internetu.

Jeżeli chodzi o system S46, to pan minister wskazał na jego zakres danych. Natomiast tytułem uzupełnienia – system też miał zbierać dane i umożliwiać ich analizę. Z naszego punktu widzenia był lub jest szansą, o ile zostanie wykonane… Pan minister wspominał o tym, że coraz więcej podmiotów jest do niego podłączanych i jeszcze będzie

podłączonych. Chodzi o szansę na szybkie zbieranie danych, przekazywanie tych danych. Nie twierdziliśmy, że system miał służyć bezpośrednio indywidualnym użytkownikom internetu. Natomiast dzięki temu, że podmioty kluczowe – szereg instytucji o takim charakterze, operatorzy telekomunikacyjni, banki – byłyby wpięte w ten system, to on zapewniałby realną szybką wymianę informacji, agregowanie tych informacji, bo to też jest bardzo ważne. Ten system mógłby się przyczynić do tego, żeby szybciej i sprawniej dostarczać aktualne informacje obywatelom poprzez inne kanały komunikowania. Dziękuję bardzo.

Przewodniczący poseł Wojciech Szarama (PiS):

Czy ktoś jeszcze chciałby zabrać głos? Pan, czy niekoniecznie… Jak pan uważa. Proszę się przedstawić.

Zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości w Komendzie Głównej Policji insp. Michał Pudło:

Inspektor Michał Pudło, zastępca komendanta Centralnego Biura Zwalczania Cyberprzestępczości.

Szanowny panie przewodniczący, szanowni panowie, bardzo dziękuję za docenienie tytanicznej pracy, jaką wykonała Policja, w zakresie powstania nie tylko CBZC, ale całego systemu zwalczania cyberprzestępczości. Oczywiście to jest dopiero początek. Jesteśmy w trakcie pewnego olbrzymiego zadania. Dziękuję za możliwość uczestnictwa w posiedzeniu.

W zakresie pytania, które zadał pan poseł, chciałem odpowiedzieć, że ustawa z 17 grudnia 2021 r., na mocy której powstało Centralne Biuro Zwalczania Cyberprzestępczości, zakładała pewne etapy powstawania biura. Pierwszy etap był 12 stycznia 2022 r., kiedy powstało biuro, następnie był półroczny okres powstania biura poprzez powołanie pełnomocnika. Biuro faktycznie zaczęło swoją działalność 12 lipca 2022 r. W pierwszym roku funkcjonowania ustawa przewiduje 300 etatów w Centralnym Biurze Zwalczania Cyberprzestępczości. W kolejnym, czyli obecnym, 800 etatów. W następnym kolejne 500, czyli 1200. I 1800 etatów w 2025 r. Tak jak powiedziałem, teraz mamy 800 etatów.

Na dzień dzisiejszy w biurze pełni służbę 483 policjantów. Odejmując to od planowanej liczby 800 etatów – jest 317 wakatów. Oczywiście trwa proces rekrutacji. Nie tylko wśród policjantów pełniących służbę w innych jednostkach Policji, ale również dla osób z tzw. cywila, którzy chcą przyjąć się do Policji. Ten proces trwa, jest na bieżąco prowadzony. Pierwsze szkolenia, jak myślę, rozpoczną się jeszcze w tym roku. Dziękuję.

Przewodniczący poseł Wojciech Szarama (PiS):

Proszę.

Poseł Przemysław Koperski (Lewica):

Panie przewodniczący, jeszcze jedno pytanie. Rozumiem, że ta praca jest wykonywana na terenie nie tylko regionu, lecz także w poszczególnych jednostkach Policji, tylko że oni są podlegli pod biuro. Czy muszą pracować w Warszawie? Jak to jest?

Zastępca komendanta CBZC w KGP insp. Michał Pudło:

Centralne Biuro Zwalczania Cyberprzestępczości przypomina trochę w strukturze Centralne Biuro Śledcze Policji. Jest centrala z siedzibą w Warszawie oraz jest zarząd terenowy lub wydział w każdym województwie. Docelowo w 2025 r. będzie zarząd w każdym województwie. Dzisiaj ze względu na mniejszą liczbę etatów w niektórych województwach są wydziały. Natomiast w większych miastach jak Katowice, Wrocław, Poznań, Łódź i Kraków są już zarządy.

Funkcjonowanie CBZC to nie tylko te etaty, o których powiedziałem. Nawiązując do wypowiedzi panów kontrolerów, à propos wysysania policjantów do naszego biura z innych jednostek Policji, staramy się szkolić policjantów w terenie. Odpowiadamy na wnioski płynące z raportu. Staramy się przeszkolić każdego policjanta w zakresie choćby możliwości prawidłowego przyjmowania zawiadomień o przestępstwie i wykonania pierwszych czynności, które mogłyby przybliżyć nas do wykrycia sprawcy. Dziękuję.

Poseł Przemysław Koperski (Lewica):

Dziękuję.

Przewodniczący poseł Wojciech Szarama (PiS):

Dziękuję bardzo. Widzę, że nie ma już więcej pytań ani zgłoszeń.

Stwierdzam, że Komisja zapoznała się z informacją na temat wyników przeprowadzonej kontroli NIK. Dziękuję państwu za udział w posiedzeniu Komisji, za przedstawienie wyników kontroli. Dziękuję państwu za dyskusję.

Zamykam posiedzenie Komisji do Spraw Kontroli Państwowej.